internetworking

**Module Description:** The intent of this Knowledge Unit is to provide students with an understanding of networking and internet protocols.

**Prerequisite Knowledge:**  Students are expected to have a familiarity with different types of networks and network devices.

**Length of Completion**: 6 lecture/meeting/active learning hours, 6 hours outside of lecture reading/preparation, homework.

**Level of Instruction:** This module intended for advanced undergraduate students majoring in computer science or computer engineering.

**Learning Setting:** This module is suitable for many forms of delivery: online/in-class/hybrid. Best delivery is in a lab class where students can explore in an active learning environment.

**Lab Environment:** A computer with Wireshark and/or tcpdump installed.

**Activity/Lab Tasks:** Learning activities involves group discussion and internet searches.

**Lab Files that are Needed:** Sample PCAP files for use with Wireshark and/or tcpdump.

# learning outcomes

MODULE learning oUTCOMES

* Students will be able to describe and discuss data network architectures and protocols.
* Students will be able to describe the ISO networking model.
* Students will be able to describe and discuss data network architectures and protocols, including UDP, TCP and IP protocols.
* Students will be able to track and identify the packets involved in a simple TCP connection (or a trace of such a connection).
* Students will be able to describe the PCAP file format.
* Students will be able to read and interpret the contents of a PCAP file.

# module Details

**Interconnection:** This module is not directly interconnected with other modules.

**Instructional Files and Online Resources that are Needed:**

* Lesson 1: Lesson\_1\_Networking\_Overview.pptx
* Lesson 2: Lesson\_2\_Internetworking.pptx
* Lesson 3: Lesson\_3\_PCAP.pptx
* Lesson 4: Network Attacks and Threats

**Assessment:** This provides a reference of what is included in the assessment guide and a mapping of how the assessment items cover all module and lesson learning outcomes.

# lessons

**Overview of Lessons**

* Lesson 1: Networking Overview
* Lesson 2: Internetworking
* Lesson 3: PCAP File format
* Lesson 4: Network Security Services, Threats and Attacks

**Lesson 1: Networking Overview**

Lesson 1 Learning Outcomes:

Upon completion of this lesson:

* Students will be able to describe and discuss data network architectures and protocols.
* Students will be able to describe the ISO networking model.

Lesson 1 Details:

**Warm Up:** Ask the students to define networking. Discuss different types of network devices. Ask about network communication, specifically on a smart phone. What types of communication exist in the smart phone? How is it coordinated.

**Lesson:** The lesson here is based on the PowerPoint slides and is a standard lecture. Allow time for questions and discussion during the lecture.

**Topics covered include:**

* Networking Overview
* Overview of OSI Model
* Overview of DoD Model

**Active Learning Activity:** N/A

**Lesson 2: Internetworking**

Lesson 2 Learning Outcomes:

Upon completion of this lesson:

* Students will be able to describe and discuss data network architectures and protocols, including UDP, TCP and IP protocols.
* Students will be able to track and identify the packets involved in a simple TCP connection (or a trace of such a connection).

Lesson 2 Details:

**Warm Up:** This lesson should take a few lectures. For the first lecture, ask about the ISO and DoD models. Focus on network layers. For subsequent lectures ask the student some questions about the previous lecture – such as features of the layers discussed.

**Lesson:** The lesson here is based on the PowerPoint slides and is a standard lecture. Allow time for questions and discussion during the lecture.

**Topics Covered:**

* Overview of Internetworking and Internetworking Services
* Internet Protocols and Their Services
  + The Internet Protocol (IP)
  + The Internet Control Message Protocol (ICMP)
* Transport Protocols and Their Services
  + User Datagram Protocol (UDP)
  + Transport Control Protocol (UDP)

**Active Learning Activity:** Have students explore sample pcap capture files using Wireshark (wireshark lab) and/or tcpdump (tcpdump lab).

**Lesson 3: PCAP**

Lesson 3 Learning Outcomes:

Upon completion of this lesson:

* Students will be able to describe the PCAP file format.
* Students will be able to take a PCAP file and read the contents of the file.

Lesson 3 Details:

**Warm Up:** Discuss Wireshark and/or tcpdump and the details found in the previous lesson. As how the programs understood the contents of the sample data files. Discuss (if relevant) need for standardization not only of protocols but of data files.

**Lesson:** The lesson here is based on the PowerPoint slides and is a standard lecture. Allow time for questions and discussion during the lecture.

**Topics Covered:**

* Pcap file format and fields
* Review of IP and TCP Headers

**Active Learning Activity:** Active learning here is a set of programming labs. First students will use hd, od, or some hexeditor to view the contents of a PCAP file. They should be able to find specific values. Second, they will write a simple program to loop through the PCAP file (don’t let them use complex libraries) counting the number of records. Third assignment will have them expand on their programs to obtain information within the PCAP records.

**Lesson 4: Network Security Services, Threats and Attacks**

Have students read the discussion of Mitnick’s attack before class

* <https://www.giac.org/paper/gsec/1929/kevin-mitnick-hacking/100826>

Lesson 4 Learning Outcomes:

Upon completion of this lesson:

* Students will be able to describe the PCAP file format.
* Students will be able to take a PCAP file and read the contents of the file.

Lesson 4 Details:

**Warm up:**

Ask students to discuss different network threats. Try to differentiate between attacks against network infrastructure (eavesdropping, wiretapping, attacks against routing protocols, ip-masquerading) and attacks against network applications/services on the network (such as attacks against web sites).

**Lesson:** The lesson here is based on the PowerPoint slides and is a standard lecture. Allow time for questions and discussion during the lecture.

**Topics Covered:**

* Network Security Services
  + Confidentiality, Integrity, Availability
* Threats

**Active Learning Activity:**

Discuss the Mitnick attack. Brainstorm possible security solutions to the network

Please attribute Dr. Jim Alves-Foss and Dr. Jia Song, University of Idaho  
  
  
  
Except where otherwise noted, this work is licensed under <https://creativecommons.org/licenses/by-nc-sa/4.0/>  
  
Notwithstanding the non-commercial license terms, non-profit educational institutions are granted a non-exclusive, royalty-free license to adapt and use this material, with attribution.  
  
Creative Commons and the double C in a circle are registered trademarks of Creative commons in the United States and other countries. Third party marks and brands are the property of their respective holders.